

CLAIMS

1. A method for verifying that data received by a receiver (2) have been sent by a transmitter (1, 3) authorized by a trusted third party, the transmitter and the receiver being connected to a digital network, characterized in that an identifier (IdEvent) is associated with the data sent by the transmitter and in that the method comprises the steps consisting, for the receiver (2), in:

- (a) generating a random number (C);
 - 10 (b) broadcasting said random number over the network;
 - (c) receiving from the transmitter a response (R) computed by applying a first function (G) to said random number (C) and to said identifier (IdEvent);
 - (d) verifying the received response (R) by applying a second
 - 15 function (H) to the received response (R), to said random number (C) and to said identifier (IdEvent);
- the first function (G) having previously been delivered to the transmitter by the trusted third party and the second function (H) being a function for verifying the result of the first function, previously delivered by
- 20 the trusted third party to the receiver.

2. The method as claimed in claim 1, in which the step (b) is replaced by a step consisting in sending said random number (C) to the transmitter.

25

3. The method as claimed in claim 1, in which the receiver also transmits said identifier (IdEvent) in the step (b).

4. The method as claimed in one of claims 1 to 3, characterized in that the receiver inhibits access to said data if the response (R) received in the step (c) is not correct or if no response is received after the expiry of a predetermined time starting from the transmission of the random number (C).

5. A method for proving that data sent to a receiver (2) have been transmitted by a transmitter (1, 3) authorized by a trusted third party, the transmitter and the receiver being connected to a digital network, characterized in that an identifier (IdEvent) is associated with the data sent

35

by the transmitter and in that the method comprises the steps consisting, for the transmitter (1, 3) in:

- (a) receiving a random number (C) from the receiver (2);
- (b) computing a response (R) by applying a first function (G) to
5 said random number (C) and to said identifier (IdEvent);
- (c) sending said response (R) to the receiver (2);
said response being likely to be verified by the receiver by
applying a second function (H) to the received response (R), to said
random number (C) and to said identifier (IdEvent);
- 10 the first function (G) having previously been delivered to the
transmitter by the trusted third party and the second function (H) being a
function for verifying the result of the first function, previously delivered by
the trusted third party to the receiver.

15 6. The method as claimed in claim 5, in which the transmitter
also receives in the step (a) said identifier (IdEvent) associated with the
data received by the receiver and in which the steps (b) and (c) are not
carried out unless said identifier received in the step (a) corresponds to the
identifier associated with the data that the transmitter has just sent.

20 7. The method as claimed in any one of the preceding claims,
characterized in that the identifier associated with the data sent by the
transmitter is a random number generated by the initial transmitter of the
data in the network and attached to said data by the initial transmitter.

25 8. The method as claimed in one of the preceding claims,
characterized in that the first function (G) is a public function using a secret
key.

30 9. The method as claimed in claim 8, characterized in that the
second function (H) is a boolean function

computing an expected response by applying to said random
number (C) and to said identifier (IdEvent) the first function (G) with the
secret key and

35 comparing the expected response with the response received in
order to deliver:

- a "0" value if the expected and received responses are
different and

- a "1" value if the expected and received responses are equal.

10. The method as claimed in one of claims 1 to 7, characterized in that the first function (G) is a secret function.

5

11. The method as claimed in claim 10, characterized in that the second function (H) is a boolean function

computing an expected response by applying the first function (G) to said random number (C) and to said identifier (IdEvent) and

10 comparing the expected response with the received response in order to deliver:

- a "0" value if the expected and received responses are different and

- a "1" value if the expected and received responses are equal.

15

12. The method as claimed in one of claims 1 to 7, characterized in that the first function (G) is a public function for signature generation with the aid of a private key.

20

13. The method as claimed in claim 12, characterized in that the second function (H) is a public function for signature verification with the aid of a public key corresponding to the private key used by the first function.